Idéaux premiers associés
et décomposition primaire

David A. Madore (`david.madore@ens.fr`)

27/10/97

1. Idéaux premiers associés.

Définition (1.1). *Soit A un anneau et M un A-module. Un idéal premier $\mathfrak{p}$ de A est appelé idéal premier associé de M lorsque $\mathfrak{p}$ est l'annulateur d'un élément (nécessairement non nul) de M. On note $\mathrm{Ass}(M)$ et on appelle assassin de M l'ensemble des idéaux premiers associés de M. Lorsque I est un idéal de A, on définit les idéaux premiers associés de I comme ceux du A-module A/I.*

Il est clair qu'un idéal premier $\mathfrak{p}$ de A est un idéal premier associé de M si et seulement si M a un sous-module isomorphe à $A/\mathfrak{p}$. En effet, si $\mathfrak{p}$ est l'annulateur de $x \in M$, on a $Ax \cong A/\mathfrak{p}$; réciproquement, si $A/\mathfrak{p} \hookrightarrow M$, l'image de 1 (ou d'ailleurs de tout élément non nul puisque $A/\mathfrak{p}$ est intègre) a $\mathfrak{p}$ pour annulateur. Remarquons que tout idéal premier associé à M contient $\mathrm{ann}(M)$.

Remarquons par ailleurs que si N est un sous-module de M, on a trivialement $\mathrm{Ass}(N) \subseteq \mathrm{Ass}(M)$.

On a $\mathrm{Ass}(0) = \varnothing$. Sur un anneau *noethérien*, la réciproque est vraie, et pour le démontrer nous avons besoin du lemme suivant :

Lemme (1.2). *Soit M un A-module, et $\mathfrak{p}$ un élément maximal pour l'inclusion parmi l'ensemble des annulateurs des éléments non nuls de M. Alors $\mathfrak{p}$ est premier, donc $\mathfrak{p} \in \mathrm{Ass}(M)$.*

Soit $\mathfrak{p} = \mathrm{ann}(x)$ un tel élément maximal. Il est clair que $\mathfrak{p} \neq A$. Remarquons aussi que pour tout $c \in A$ tel que $cx \neq 0$, on a $\mathrm{ann}(cx) \supseteq \mathrm{ann}(x)$ donc $\mathrm{ann}(cx) = \mathfrak{p}$. Soient maintenant $a, b \in A$ tels que $ab \in \mathfrak{p}$. Ainsi, $abx = 0$, mais alors soit b annule $x \neq 0$, soit a annule $bx \neq 0$. Dans le premier cas, $b \in \mathrm{ann}(x) = \mathfrak{p}$; dans le second, $a \in \mathrm{ann}(bx) = \mathfrak{p}$. Ce qu'il fallait démontrer.

On en déduit aussitôt la

Proposition (1.3). *Soit A un anneau noethérien et $M \neq 0$ un A-module. Alors $\mathrm{Ass}(M) \neq \varnothing$.*

Et par ailleurs le même lemme nous permet de montrer

Proposition (1.4). *Soit A un anneau noethérien et M un A-module. Alors l'union des idéaux premiers associés de M est exactement l'ensemble de homothéties non injectives sur M (c'est-à-dire des $a \in A$ tels que $ax = 0$ pour un $x \neq 0$ de M).*

Si a est dans un idéal premier associé $\mathfrak{p}$ de M, alors $\mathfrak{p}$ est l'annulateur d'un $x \in M \setminus \{0\}$ et donc $ax = 0$. Réciproquement, si $ax = 0$ avec $x \in M \setminus \{0\}$, on a $a \in \mathrm{ann}(x)$, et le lemme montre que $\mathrm{ann}(x)$ est contenu dans un idéal premier associé de M.

Proposition (1.5). *Soit $0 \to M' \to M \to M'' \to 0$ une suite exacte de modules sur un anneau A. Alors*

$$\mathrm{Ass}(M') \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$$

Nous avons déjà signalé la première inclusion. Prouvons la seconde : soit $\mathfrak{p} \in \mathrm{Ass}(M)$. Alors il existe un sous-module N de M isomorphe à $A/\mathfrak{p}$. S'il existe un élément non nul x dans $N \cap M'$ (on identifie M' a son image dans M), alors l'annulateur de x est $\mathfrak{p}$ (puisque $A/\mathfrak{p}$ est un anneau intègre), donc $\mathfrak{p} \in \mathrm{Ass}(M')$. En revanche, si $N \cap M' = 0$, alors N s'envoie isomorphiquement dans M'' donc $\mathfrak{p} \in \mathrm{Ass}(M'')$.

Proposition (1.6). *Si $(M_i)_{i\in I}$ est une famille de A-modules, alors $\mathrm{Ass}(\bigoplus_i M_i) = \bigcup_i \mathrm{Ass}(M_i)$.*

On se ramène au cas où I est fini en constatant que tout élément de la somme directe des M_i appartient déjà à la somme directe d'un nombre fini des M_i (et y a le même annulateur). Par récurrence sur le cardinal de I, on se ramène au cas de deux modules : $M = M' \oplus M''$. Alors la proposition précédente montre que $\mathrm{Ass}(M') \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$ et $\mathrm{Ass}(M'') \subseteq \mathrm{Ass}(M) \subseteq \mathrm{Ass}(M') \cup \mathrm{Ass}(M'')$, d'où le résultat.

Théorème (1.7) ("dévissage"). *Soit M un module de type fini sur un anneau noethérien A. Alors il existe une suite*

$$0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$$

telle que pour tout i on ait $M_{i+1}/M_i \cong A/\mathfrak{p}_i$ avec $\mathfrak{p}_i$ un idéal premier.

On construit les M_i par récurrence sur i. On pose $M_0 = 0$. Si $M/M_i \neq 0$, alors il existe, d'après la proposition (1.3), un idéal premier associé $\mathfrak{p}_i$ de M/M_i, et donc un sous-module M_{i+1} de M tel que $M_{i+1}/M_i \cong A/\mathfrak{p}_i$. La suite de modules (M_i) est croissante, et comme M est noethérien, elle est stationnaire, donc il existe n tel que $M_n = M$, et la construction s'arrête là.

Il n'est pas toujours vrai qu'on peut trouver une telle suite où les $\mathfrak{p}_i$ soient de plus des idéaux premiers associés de M. (Les modules M pour lesquels c'est possible s'appellent "clean" en anglais.) Par ailleurs, les $\mathfrak{p}_i$ ne sont pas uniquement déterminés.

En revanche, on remarquera que d'après la proposition (1.5), tous les idéaux premiers associés de M sont parmi les $\mathfrak{p}_i$. Ceci nous démontre au passage le

Corollaire (1.8). *Soit M un module de type fini sur un anneau noethérien A. Alors $\mathrm{Ass}(M)$ est fini.*

2. Idéaux premiers associés et localisation.

Proposition (2.1). *Soit A un anneau noethérien, et S une partie multiplicative de A. Alors pour tout A-module M, l'assassin de $S^{-1}M$ est exactement l'ensemble des $S^{-1}\mathfrak{p}$ pour $\mathfrak{p} \in \mathrm{Ass}_A M$ ne rencontrant pas S.*

Si $\mathfrak{p} \in \mathrm{Ass}_A M$ ne rencontre pas S, alors $S^{-1}\mathfrak{p}$ est un idéal premier de $S^{-1}A$. De plus, comme on a une injection $A/\mathfrak{p} \hookrightarrow M$, on en déduit par localisation une injection $(S^{-1}A)/(S^{-1}\mathfrak{p}) \hookrightarrow S^{-1}M$ (par exactitude de la localisation). Ainsi, $S^{-1}\mathfrak{p}$ est dans $\mathrm{Ass}_{S^{-1}A}\, S^{-1}M$. (Remarquons que cette partie n'utilise pas le fait que A est noethérien.)

Réciproquement, si $\mathfrak{q}$ est un idéal premier associé du $S^{-1}A$-module $S^{-1}M$, on sait qu'on peut écrire $\mathfrak{q} = S^{-1}\mathfrak{p}$ avec $\mathfrak{p}$ un idéal premier de A ne rencontrant pas S. Supposons que $\mathfrak{q}$ soit l'annulateur d'un $x \in S^{-1}M$: on peut sans perte de généralité supposer que x est dans l'image de M. Soient $a_1, \ldots, a_n$ des générateurs de $\mathfrak{p}$ (ce qui est possible puisque A est noethérien), de sorte qu'on a $s_i a_i x = 0$ pour des $s_i \in S$. Si on pose $s = s_1 \cdots s_n$, on a alors $sax = 0$ pour tout $a \in \mathfrak{p}$. Ainsi, $\mathfrak{p}$ contient l'annulateur de sx dans M. Mais d'autre part, tout élément de A qui annule sx dans M l'annule aussi dans $S^{-1}M$, donc annule x dans $S^{-1}M$, et est donc dans $\mathfrak{p}$. Ceci montre $\mathfrak{p} = \mathrm{ann}_M(sx)$, ce qu'il fallait démontrer.

Rappelons que pour un module M sur un anneau A, on appelle support de M et on note $\mathrm{Supp}(M)$ l'ensemble des idéaux premiers $\mathfrak{p}$ de A tels que $M_{\mathfrak{p}} \neq 0$.

Proposition (2.2). *Soit M un module sur un anneau noethérien A. Alors $\mathrm{Ass}(M) \subseteq \mathrm{Supp}(M)$ et ces deux ensembles ont les mêmes éléments minimaux.*

Si $\mathfrak{p} \in \mathrm{Ass}(M)$, alors d'après la proposition (2.1), en notant $S = A \setminus \mathfrak{p}$, on a $S^{-1}\mathfrak{p} \in \mathrm{Ass}_{S^{-1}A}(S^{-1}M)$. Mais ceci signifie que $S^{-1}M = M_\mathfrak{p}$ est non nul, donc $\mathfrak{p} \in \mathrm{Supp}(M)$.

Pour montrer que $\mathrm{Ass}(M)$ et $\mathrm{Supp}(M)$ ont les mêmes éléments minimaux, il suffit alors de montrer que tout élément $\mathfrak{p}$ de $\mathrm{Supp}(M)$ contient un élément de $\mathrm{Ass}(M)$. Notons encore $S = A \setminus \mathfrak{p}$. Alors par définition $S^{-1}M = M_\mathfrak{p}$ est non nul, et par la proposition (1.3) il existe un idéal premier associé de $S^{-1}M$ (comme $S^{-1}A$-module), lequel s'écrit $S^{-1}\mathfrak{q}$ d'après la proposition (2.1), avec $\mathfrak{q}$ un élément de $\mathrm{Ass}(M)$ disjoint de S, c'est-à-dire contenu dans $\mathfrak{p}$, ce qu'il fallait démontrer.

Remarques : (1) Si M est un A-module, où A est un anneau noethérien, alors M s'injecte dans $\prod_{\mathfrak{p} \in \mathrm{Ass}(M)} M_\mathfrak{p}$; en particulier, pour montrer qu'un élément de M est nul, il suffit de montrer qu'il se localise en zéro en les éléments de $\mathrm{Ass}(M)$ (plutôt qu'en tout idéal premier de A).

(2) Sous les hypothèses et notations du théorème (1.7), les éléments minimaux parmi les $\mathfrak{p}_i$ coïncident également avec les éléments minimaux de $\mathrm{Ass}(M)$ ou $\mathrm{Supp}(M)$. De plus, un élément $\mathfrak{p}$ de $\mathrm{Supp}(M)$ est minimal si et seulement si $M_\mathfrak{p}$ est de longueur finie[*], et alors cette longueur est le cardinal de $\{i : \mathfrak{p}_i = \mathfrak{p}\}$.

3. Modules primaires et décomposition primaire.

Définition (3.1). *Un module M non nul sur un anneau A est dit coprimaire lorsque toute homothétie non injective sur M est nilpotente. Lorsque $\mathfrak{p}$ est l'idéal formé des homothéties nilpotentes sur M, on dit que M est $\mathfrak{p}$-coprimaire. Un sous-module N d'un module M est dit [$\mathfrak{p}$-]primaire (par rapport à M) lorsque M/N est [$\mathfrak{p}$-]coprimaire. En particulier, un idéal I est dit [$\mathfrak{p}$-]primaire lorsque A/I est [$\mathfrak{p}$-]coprimaire.*

Avec les notations ci-dessus, on remarque que $\mathfrak{p}$ est nécessairement premier ; en effet, la composée de deux homothéties injectives est injective.

Dire qu'un idéal propre I est primaire revient à dire que si $a, b \in A$ avec $b \notin I$ mais $ab \in I$, alors $a \in \sqrt{I}$. En particulier, les idéaux premiers sont primaires, et tout idéal primaire radical est premier. De plus, si I est primaire, il est $\mathfrak{p}$-primaire où $\mathfrak{p} = \sqrt{I}$ est sa racine. Naturellement, si I est primaire alors $\sqrt{I}$ est premier ; la réciproque n'est cependant pas vraie, comme le contre-exemple $I = (x^2, xy) \subseteq k[x, y]$ le prouve : $\sqrt{I} = (x)$ est premier, mais I n'est pas primaire (puisque $xy \in I$ alors que $x \notin I$ et $y \notin \sqrt{I}$).

Proposition (3.2). *Soit A un anneau noethérien. Alors un A-module M de type fini est coprimaire si et seulement si $\mathrm{Ass}(M)$ est réduit à un seul élément, $\mathfrak{p}$, qui est alors la racine de $I = \mathrm{ann}(M)$, et de plus I et M sont $\mathfrak{p}$-primaire et $\mathfrak{p}$-coprimaire respectivement.*

Supposons $\mathrm{Ass}(M) = \{\mathfrak{p}\}$. Alors d'après la proposition (2.2), $\mathrm{Supp}(M)$ est l'ensemble des idéaux premiers de A contenant $\mathfrak{p}$. Or on sait que $\mathrm{Supp}(M)$ est l'ensemble des idéaux premiers contenant I. Ceci montre $\mathfrak{p} = \sqrt{I}$. Sachant que $\mathfrak{p}$ est l'ensemble des homothéties non injectives de M (proposition (1.4)) et que $\sqrt{I}$ est l'ensemble des homothéties nilpotentes de M, on a l'implication "si" et le fait que M est $\mathfrak{p}$-primaire.

[*] Un module M est dit de longueur finie n lorsqu'il existe une suite $0 = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n = M$ avec M_{i+1}/M_i simple, c'est-à-dire isomorphe à $A/\mathfrak{m}$, où $\mathfrak{m}$ est un idéal maximal. Le théorème de Jordan-Hölder assure que la longueur d'un module de longueur finie est bien définie.

À présent, si M est coprimaire et $\mathfrak{p} \in \mathrm{Ass}(M)$, alors tout $a \in \mathfrak{p}$ est une homothétie non injective, donc appartient à $\sqrt{I}$ par hypothèse. Ainsi $\mathfrak{p} \subseteq \sqrt{I}$. Mais d'autre part, il est évident que $I \subseteq \mathfrak{p}$, et donc $\sqrt{I} \subseteq \mathfrak{p}$. On a donc $\mathfrak{p} = \sqrt{I}$ et $\mathrm{Ass}(M) = \{\sqrt{I}\}$ (puisque $\mathrm{Ass}(M)$ est non vide, proposition (1.3)).

Montrons enfin que dans ces circonstances, I est ($\mathfrak{p}$-)primaire. Si $a, b \in A$ vérifient $ab \in I$ mais $b \notin I$, alors $abM = 0$ mais $bM \neq 0$, donc a est une homothétie non injective sur M, et comme on l'a vu ceci implique $a \in \sqrt{I}$, ce qu'il fallait démontrer.

Remarque : La définition d'un module primaire que nous avons donnée est celle trouvée dans [Mat] (mis à part que nous ne considérons pas qu'un module est primaire par rapport à lui-même) ou [Lan]. On trouve dans [Bou] une définition légèrement différente : un sous-module N d'un module M sur un anneau noethérien A est dit primaire lorsque toute homothétie a de M/N non injective est *presque nilpotente* dans le sens que pour tout $x \in M/N$ il existe $n(x) \in \mathbb{N}$ tel que $a^{n(x)}(x) = 0$. Ceci a l'intérêt de permettre d'étendre quelques résultats à des modules qui ne sont pas de type fini. Mais dans le cas réellement intéressant des modules de type fini sur un anneau noethérien, les deux définitions coïncident.

Proposition (3.3). *Si $N_1, \ldots, N_k$ sont des sous-modules $\mathfrak{p}$-primaires d'un module M sur un anneau A, alors $N_1 \cap \cdots \cap N_k$ est $\mathfrak{p}$-primaire.*

Soit $N = N_1 \cap \cdots \cap N_k$, et soit $a \in \mathfrak{p}$: alors il existe des n_i tel que $a^{n_i} x \in N_i$ pour tout $x \in M$, et si $n = \max_{i=1}^{k} n_i$, on a $a^n x \in N$ pour tout $x \in M$, donc l'homothétie de rapport a est nilpotente sur M/N. Si $a \notin \mathfrak{p}$ et $x \notin N$, il existe i tel que $x \notin N_i$, et alors $ax \notin N_i$ donc $ax \notin N$, donc l'homothétie de rapport a est injective sur M/N.

Définition (3.4). *Si M est un A-module, et que N est un sous-module de M, une <u>décomposition primaire</u> de N (dans M) est une écriture $N = \bigcap_{i \in I} M_i$ avec I fini et chaque M_i un sous-module $\mathfrak{p}_i$-primaire de M pour un certain idéal premier $\mathfrak{p}_i$ de A. Si les $\mathfrak{p}_i$ sont deux-à-deux distincts et que tous les M_i sont nécessaires (i.e. que pour tout j, $\bigcap_{i \neq j} M_i$ est strictement plus grand que N), on dit que la décomposition primaire en question est <u>réduite</u>. Les éléments minimaux pour l'inclusion parmi les $\mathfrak{p}_i$ sont dits <u>isolés</u>, les autres sont dits <u>immergés</u>.*

En faisant usage de la proposition (3.3) et en retirant les sous-modules superflus, il est clair qu'à partir d'une décomposition primaire on peut en obtenir une réduite.

Le résultat principal concernant les décompositions primaires est le suivant, pour la démonstration duquel nous renvoyons le lecteur à [Bou], [Eis], [Lan] ou [Mat] :

Théorème (3.5). *Soit M un module de type fini sur un anneau noethérien A. Alors pour tout sous-module N de M,*

(i) N admet une décomposition primaire.

(ii) Si $N = \bigcap_{i \in I} M_i$ est une décomposition primaire réduite de N, avec M_i un sous-module $\mathfrak{p}_i$-primaire pour tout i, alors les $\mathfrak{p}_i$ sont précisément les idéaux premiers associés à M ; en particulier, ils sont uniquement déterminés, et le nombre de termes d'une décomposition primaire réduite est également déterminé.

(iii) De plus, avec les notations du (ii), pour tout i tel que $\mathfrak{p}_i$ soit isolé, M_i est le noyau de $M/N \to (M/N)_{\mathfrak{p}_i}$ (i.e. l'ensemble des éléments de M envoyés dans N par un élément de A qui n'est pas dans $\mathfrak{p}_i$) ; en particulier, ces M_i sont déterminés : on les appelle les <u>composantes primaires</u> correspondant aux idéaux premiers isolés.

Pour résumer : la décomposition primaire réduite existe, fait intervenir exactement les idéaux premiers associés, et les composantes primaires correspondant aux idéaux premiers isolés sont déterminés.

Le théorème (3.5) est particulièrement important dans le cas où $M = A$ et N est un idéal. Dans le cas d'un idéal *radical*, on a le résultat beaucoup plus simple suivant :

Corollaire (3.6). *Soit $\mathfrak{r}$ un idéal radical d'un anneau noethérien A. Alors il existe des idéaux premiers $(\mathfrak{p}_i)_{i\in I}$ (I fini) tels que $\mathfrak{r} = \bigcap_{i\in I} \mathfrak{p}_i$, avec $\mathfrak{p}_j \not\supseteq \bigcap_{i\neq j} \mathfrak{p}_i$ pour tout j. De plus, les $\mathfrak{p}_i$ sont alors uniquement déterminés à permutation près.*

Au vu du théorème (3.5), la seule chose à montrer est que les $\mathfrak{p}_i$ sont radicaux (car on sait déjà qu'ils sont primaires et un idéal primaire radical est premier). Supposons donc $x^k \in \mathfrak{p}_j$. Comme $\mathfrak{p}_j \not\supseteq \bigcap_{i\neq j} \mathfrak{p}_i$, on peut trouver $y \in \bigcap_{i\neq j} \mathfrak{p}_i$ tel que $y \notin \mathfrak{p}_j$. Alors $x^k y^k \in \mathfrak{r}$, donc $xy \in \mathfrak{r}$. En particulier, $xy \in \mathfrak{p}_j$. Mais alors soit $x \in \mathfrak{p}_j$, et on a fini, soit $y \in \sqrt{\mathfrak{p}_j}$. Mais cela n'est pas possible car sinon il existe ℓ tel que $y^\ell \in \mathfrak{p}_j$, et alors $y^\ell \in \mathfrak{r}$, donc $y \in \mathfrak{r} \subseteq \mathfrak{p}_j$, une contradiction.

Si $\mathfrak{m}$ est un idéal maximal d'un anneau noethérien A, et I un idéal propre contenant $\mathfrak{m}^n$ pour un certain n, alors I est $\mathfrak{m}$-primaire. En effet, $\mathfrak{m}$ est le seul idéal premier contenant $\mathfrak{m}^n$ (car un tel idéal doit contenir $\mathfrak{m}$, donc lui être égal), donc aussi le seul idéal premier contenant I, lequel est l'annulateur de A/I. Ainsi, $\mathrm{Supp}(A/I) = \{\mathfrak{m}\}$ et on applique la proposition (2.2). En particulier, si $\mathfrak{m}$ est maximal alors $\mathfrak{m}^n$ est $\mathfrak{m}$-primaire pour tout n. Par ailleurs, un idéal premier $\mathfrak{p}$ est $\mathfrak{p}$-primaire. Cependant, les puissances d'un idéal premier ne sont pas toujours primaires, et tout idéal primaire n'est pas une puissance d'un idéal premier. Si $\mathfrak{p}$ est premier et $n \geq 1$, alors $\mathfrak{p}$ est minimal parmi les idéaux premiers contenant $\mathfrak{p}^n$, et on peut donc considérer la composante $\mathfrak{p}$-primaire de $\mathfrak{p}^n$. Celle-ci s'appelle la puissance symbolique n-ième de $\mathfrak{p}$ et se note $\mathfrak{p}^{(n)}$. On a $\mathfrak{p}^{(n)} = \mathfrak{p}^n A_{\mathfrak{p}} \cap A$.

Nous terminons par un exemple typique. Soit $A = k[x, y]$ l'anneau des polynômes à deux indéterminées sur un corps k, et $I = (x^2, xy)$. Les éléments de I sont les fonctions qui s'annulent sur l'axe des ordonnées et qui ont un zéro d'ordre 2 à l'origine : cett description donne la décomposition primaire $I = (x) \cap (x^2, xy, y^2)$. Mais on peut aussi écrire $I = (x) \cap (x^2, y)$, ce qui revient à dire que les éléments de I sont les fonctions qui s'annulent sur l'axe des ordonnées et dont la dérivée partielle par rapport à x s'annule à l'origine. Ici, les idéaux premiers associés de I sont l'idéal premier isolé (x) et l'idéal maximal plongé (x, y). Au passage, notons que l'idéal primaire (x^2, y), de racine (x, y), n'est ni une puissance ni une puissance symbolique de celle-ci.

Bibliographie.

[Bou] Nicolas Bourbaki, *Éléments de Mathématique*, Algèbre commutative, chapitre IV (idéaux premiers associés et décomposition primaire), Hermann.

[Eis] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, Graduate Texts in Mathematics 150.

[Lan] Serge Lang, *Algebra*, Addison-Wesley.

[Mat] Hideyuki Matsumura, *Commutative ring theory*, Cambridge University Press, Cambridge Studies in Advanced Mathematics.

[Ser] Jean-Pierre Serre, *Algèbre locale, multiplicités*, Springer-Verlag, Lecture Notes in Mathematics 11.